

**UNITED STATES DISTRICT COURT
DISTRICT OF MARYLAND
Northern Division (Baltimore)**

SPYRO STAMAT, individually and
on behalf of all others similarly situated,

Plaintiff,

v.

GRANDIZIO WILKINS LITTLE &
MATTHEWS, LLP
8370 Veterans Highway, Suite 104
Millersville, MD 21108,

Serve: Registered Agent:
Harry T. Wilkins
8370 Veterans Highway, Suite 104
Millersville, MD 21108

Defendant.

Case No. _____

JURY DEMAND

CONSUMER CLASS ACTION COMPLAINT

Plaintiff SPYRO STAMAT (“Plaintiff”) brings this Class Action Complaint against GRANDIZIO WILKINS LITTLE & MATTHEWS, LLP (“Defendant” or “GWLM”), in his individual capacity and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and her counsels’ investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. This class action arises out of the recent data breach (“Data Breach”) involving Defendant, a domestic for-profit accounting firm with locations around Baltimore and Annapolis, Maryland.

2. GWLM failed to reasonably secure, monitor, and maintain Personally Identifiable Information (“PII”) provided by consumers, including, without limitation, names, Social Security numbers, driver’s license numbers, medical information, and financial account information, and

of consumers stored on its private network. As a result, Plaintiff and other consumers suffered present injury and damages in the form of identity theft, loss of value of their PII, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the unauthorized access, exfiltration, and subsequent criminal misuse of their sensitive and highly personal information.

3. Moreover, after learning of the Data Breach, Defendant waited over seven months (from June 7, 2021 to January 14, 2022) to notify Plaintiff and Class Members of the Data Breach and/or inform them that their PII was compromised. During this time, Plaintiff and Class Members were unaware that their sensitive PII had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm.

4. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. Defendant's conduct in breaching these duties amounts to negligence and/or recklessness and violates federal and state statutes.

5. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to take reasonable steps to protect the PII of Plaintiff and Class Members and warn Plaintiff and Class Members of Defendant's inadequate information security practices. Defendant disregarded the rights of Plaintiff and Class Members by knowingly failing to implement and maintain adequate and reasonable measures to ensure that the PII of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized

disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use.

6. As a direct and proximate result of Defendant's data security failures and the Data Breach, the PII of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party, and Plaintiff and Class Members have suffered actual, present, concrete injuries. These injuries include: (i) the current and imminent risk of fraud and identity theft (ii) lost or diminished value of PII ; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iv) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; and (v) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII; (vi) the invasion of privacy; (vii) the compromise, disclosure, theft, and unauthorized use of Plaintiff's and the Class Members' PII; and (viii) emotional distress, fear, anxiety, nuisance and annoyance related to the theft and compromise of their PII.

7. Plaintiff and Class Members seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and remains at risk due to inadequate data security.

8. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

Plaintiff Spyro Stamat

9. Plaintiff Spyro Stamat is, and at all times relevant has been, a resident and citizen of Delaware, where he intends to remain. Plaintiff received a “Notice of Data Security Incident” letter dated January 14, 2022, on or about that date.

10. The letter notified Plaintiff that on June 7, 2021, GWLM discovered unauthorized access to a GWLM employee’s email account.

11. After an investigation, GWLM determined that Plaintiff’s information was compromised in the Data Breach by the unauthorized access. The files subject to unauthorized access contained Plaintiff’s and Class Members’ names, Social Security numbers, driver’s license numbers, medical information, and financial account information.

12. The letter further advised Plaintiff that he should spend time mitigating his losses by taking steps to help safeguard his information, including following recommendations by the Federal Trade Commission regarding identity theft protection and placing a fraud alert or security freeze on his credit file.

13. The letter also encouraged Plaintiff to sign up for one year of credit and identity monitoring through IDX. Upon information and belief, the credit and identity monitoring offered is only single bureau credit monitoring.

14. Defendant obtained and continues to maintain Plaintiff’s and Class Members’ PII and has a continuing legal duty and obligation to protect that sensitive information from unauthorized access and disclosure. Plaintiff would not have entrusted his PII to Defendant had he known that it would fail to maintain adequate data security. Plaintiff’s PII was compromised and disclosed as a result of the Data Breach.

Defendant Grandizio Wilkins Little & Matthews

15. Defendant GWLM is Maryland corporation with a principal office location of 8370 Veterans Highway, Suite 104, Millersville, MD 21108.

16. Defendant GWLM is a full-service accounting firm, offering a broad range of tax and business services for business owners and independent professionals. It operates out of two locations – one in Sparks, Maryland and another in Millersville, Maryland.

17. All of Plaintiff's claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

18. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of \$5,000,000 exclusive of interest and costs, there are more than 100 putative class members, and minimal diversity exists because many putative class members are citizens of a different state than Defendant. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

19. This Court has personal jurisdiction over GWLM because it is headquartered in and maintains its principal place of business in this District. GWLM is authorized to and regularly conducts business in Maryland. In this District, GWLM makes decisions regarding corporate governance and management of its businesses, including decisions regarding the security measures to protect its customers' PII. GWLM intentionally avails itself of this jurisdiction by promoting, selling and marketing its services from Maryland to thousands of consumers in Maryland and other states. Venue is proper in this District under 28 U.S.C. § 1391(a) through (d) because GWLM's headquarters and principal place of business are located in this District, GWLM resides in this

District, and substantial parts of the events or omissions giving rise to the claims occurred in or emanated from this District, including, without limitation, decisions made by GWLM's governance and management personnel or inaction by those individuals that led to misrepresentations, invasions of privacy, and the Data Breach.

IV. FACTUAL ALLEGATIONS

Background

20. Defendant is a full-service accounting firm, offering not only tax preparation and tax planning services, but also a wide-range of business services, including audits, strategic business planning, new business formation, cash flow management, business valuation, and succession planning.

21. Plaintiff and Class Members were persons who provided, or who third-parties provided on their behalf, their PII to Defendant in conjunction with utilizing GWLM's tax and business services.

22. Plaintiff and Class Members relied on the sophistication of Defendant and its network to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand security to safeguard their PII.

23. Defendant required the submission of and voluntarily accepted the PII as part of its business and had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties. GWLM has a legal duty to keep consumer's PII safe and confidential.

24. The information held by Defendant in its computer systems and networks (including its employee email accounts) included the unencrypted PII of Plaintiff and Class Members.

25. Defendant derived a substantial economic benefit from collecting Plaintiff's and Class Members' PII. Without the required submission of PII, GWLM could not perform the services it provides.

26. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, GWLM assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

27. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII.

The Data Breach

28. On June 7, 2021, Defendant discovered unauthorized access to a GWLM employee's email account.

29. According to Defendant, it took unidentified steps to secure its email system, and then allegedly launched an investigation into the matter. Defendant allegedly "immediately engaged cybersecurity experts to determine if information had been affected."

30. To date, GWLM has not revealed most (if not all) of the findings of the investigation it commissioned. GWLM has not revealed when the unauthorized actor first gained access to a GWLM employee email account, nor has it revealed the mechanism by which the unauthorized actor first gained access to a GWLM employee email account. GWLM has not revealed whether additional employee email accounts were subsequently breached, or whether the unauthorized

actor was able to access GWLM's broader computer network via the unauthorized access to an employee email account.

31. Even worse, GWLM has failed to disclose the exact nature of the unauthorized access to Plaintiff's and Class Members' PII. Instead, GWLM speaks in generalities and equivocations, claiming that it only knows that Plaintiff's PII "may have been involved," that files "may have been accessed by the unauthorized individual," and that those files "may have contained names, Social Security numbers, Medical Information, Drivers License Information, Financial Account Information, or Payment Card Information."

32. This "disclosure" amounts to no real disclosure at all, as it fails to inform Plaintiff and Class Members what information belonging to them was affected, leaving Plaintiff and Class Members to believe that all of this incredibly sensitive PII was compromised in this Data Breach.

33. Defendant's offering of credit and identity monitoring also belies GWLM's equivocal statements that Plaintiff's and Class Members' PII "may have been affected," and instead establishes that Plaintiff's and Class Members' sensitive PII was in fact affected, accessed, compromised, and exfiltrated from Defendant's computer systems.

34. Upon information and belief, the unauthorized actor gained access to GWLM's employee email account well in advance of the June 7, 2021 date that the intrusion was first discovered by GWLM, meaning that the unauthorized actor had unfettered and undetected access to Defendant's networks for a considerable period of time prior to GWLM becoming aware of the unauthorized access to its email accounts, computer systems, and network.

35. The investigation commissioned by GWLM did not conclude until December 17, 2021, and notice was not sent to victims of the data breach until nearly a month after that. Thus, the victims of this Data Breach, including Plaintiff and Class Members, were not sent notice of

this Data Breach until approximately seven (7) months after GWLM first knew about this Data Breach.

36. Defendant's investigation was inconclusive whether or not the accessed data has been or will be misused by the hackers. However, upon information and belief, GWLM has no methods, policies, or procedures in place that would afford its customers (like Plaintiff and Class Members) any mechanism or opportunity to report misuse of the data back to GWLM, and the investigation commissioned by GWLM did not survey GWLM's clients whose data was breached for evidence of misuse.

37. The attacker accessed and acquired files in employee email accounts containing unencrypted PII of Plaintiff and Class Members, including names, Social Security numbers, Medical Information, Driver's License Information, Financial Account Information, or Payment Card Information.

38. On or around January 14, 2022, Defendant also disclosed the Data Breach to multiple States' Attorney Generals.

39. GWLM first notified its impacted consumers of the incident on or around January 14, 2022, sending written notifications to individuals whose personal information was compromised in the Data Breach.

40. Plaintiff's and Class Members' PII was accessed and stolen in the Data Breach.

41. Plaintiff further believes his PII, and that of Class Members, was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type

42. To prevent and detect cyber-attacks attacks Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

43. To prevent and detect cyber-attacks Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks....
- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)....
- **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it....
- **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic....¹

44. To prevent and detect cyber-attacks attacks Defendant could and should have

¹ See Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at*: <https://us-cert.cisa.gov/ncas/tips/ST19-001> (last visited Nov. 11, 2021).

implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].²

² See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at*: <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/> (last visited Nov. 11, 2021).

45. Upon information and belief, Defendant also transmitted and stored unencrypted PII in employee emails, a grossly negligent act.

46. Given that Defendant was storing the PII of Plaintiff and Class Members, Defendant could and should have implemented all of the above measures to prevent and detect cyber-attacks.

47. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent what appears to be an email phishing attack (which is the most common and easily thwarted form of cyberattack), resulting in the Data Breach and the exposure of the PII of an undisclosed amount of current and former consumers, including Plaintiff and Class Members.

Defendant Acquires, Collects, and Stores the PII of Plaintiff and Class Members

48. Defendant acquired, collected, and stored the PII of Plaintiff and Class Members.

49. Defendant retains and stores this information, and derives a substantial economic benefit from the PII that it collects. But for the collection of Plaintiff's and Class Members' PII, Defendant would be unable to perform its tax and business services.

50. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII from disclosure.

51. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendant to keep their PII confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

52. Defendant could have prevented this Data Breach by instituting policies and practices not to transmit or store unencrypted PII in employee email account, or by properly

securing and encrypting the emails, files and file servers containing the PII of Plaintiff and Class Members.

53. Defendant's policies on its website include promises and legal obligations to maintain and protect PII, demonstrating an understanding of the importance of securing PII. In fact, GWLM's website unequivocally states that:

Security is very important to us. We don't just consider security on our end, we think about yours as well.

We send all sensitive documentation through Citrix ShareFile to ensure the information is sent to your securely. We also encourage our clients to do the same when sending files to use.³

54. Defendant also has adopted a Privacy Policy that details specific privacy obligations and promises to its customers, including Plaintiff and Class Members.⁴

55. Defendant's negligence in safeguarding the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

56. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

This Email Phishing Attack Was Completely Foreseeable.

57. While Defendant has been purposefully vague about the mechanism of this cyberattack, upon information and belief, this Data Breach occurred as the result of a targeted email phishing attack. The targeted email phishing attack against Defendant was completely foreseeable.

58. According to Verizon, over 90% of all cybersecurity attacks that result in a data

³ <https://www.gwlmcpa.com/custom7.php> (last accessed March 22, 2022)

⁴ <https://www.gwlmcpa.com/privacy.php> (last accessed March 22, 2022)

breach start with a phishing attack.⁵

59. “Phishing is a cyber-attack that uses disguised email as a weapon. In simple terms, phishing is a method of obtaining personal information using deceptive e-mails and websites. The goal is to trick the email recipient into believing that the message is something they want or need — a request from their bank, for instance, or a note from someone in their company — and to click a link or download an attachment.”⁶ The fake link will typically mimic a familiar website and require the input of credentials. Once input, the credentials are then used to gain unauthorized access into a system.

60. Phishing attacks are among the oldest, most common, and well known form of cyberattack. “It’s one of the oldest types of cyberattacks, dating back to the 1990s” and one that every organization with an internet presence is aware.”⁷ It remains the “simplest kind of cyberattack and, at the same time, the most dangerous and effective.”⁸

61. Phishing attacks are well understood by the cyber-protection community and are generally preventable with the implementation of a variety of proactive measures such as

⁵ *Verizon Says Phishing Drives 90% of Cybersecurity Breaches*, Graphus (Jan. 21, 2020), <https://www.graphus.ai/verizon-says-phishing-still-drives-90-of-cybersecurity-breaches/>.

⁶ Josh Fruhlinger, *What is Phishing? How This Cyber-Attack Works and How to Prevent It*, CSO Online (Sept. 4, 2020), <https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html>

⁷ *What is phishing? How this cyber attack works and how to prevent it*, CSO Online, February 20, 2020, <https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html> (last visited October 28, 2020).

⁸ *Phishing*, Malwarebytes, <https://www.malwarebytes.com/phishing/> (last visited October 28, 2020).

sandboxing inbound e-mail⁹, inspecting and analyzing web traffic, penetration testing¹⁰, and employee education, among others.

62. As a sophisticated commercial entity that collects and stores a plethora of PII, an email phishing attack, and the potential harms arising therefrom, was reasonably foreseeable to Defendant.

Defendant Knew or Should Have Known of the Risk Because the Accounting Sector is Particularly Susceptible to Cyber Attacks

63. Defendant knew and understood unprotected or exposed PII in the custody of accounting firms such as Defendant is valuable and highly sought after by nefarious third parties seeking to illegally monetize that PII through unauthorized access, as accounting firms maintain highly sensitive PII, including Social Security numbers and financial information.

64. Moreover, it has been well-reported that the banking/credit/financial services industry is one of the most “at-risk” industries when it comes to cybersecurity attacks.¹¹ Attacks against the financial sector increased 238% globally from the beginning of February 2020 to the end of April, with some 80% of financial institutions reporting an increase in cyberattacks, according to cyber security firm VMware.

⁹ Sandboxing is an automated process whereby e-mail with attachments and links are segregated to an isolated test environment, or a “sandbox,” wherein a suspicious file or URL may be executed safely.

¹⁰ Penetration testing is the practice of testing a computer system, network, or web application to find security vulnerabilities that an attacker could exploit. The main objective of penetration testing is to identify security weaknesses. Penetration testing can also be used to test an organization’s security policy, its adherence to compliance requirements, its employees’ security awareness and the organization’s ability to identify and respond to security incident. The primary goal of a penetration test is to identify weak spots in an organization’s security posture, as well as measure the compliance of its security policy, test the staff’s awareness of security issues and determine whether - and how -- the organization would be subject to security disasters. See <https://searchsecurity.techtarget.com/definition/penetration-testing> (last visited October 28, 2020).

¹¹ See, e.g., <https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/financial-services-risk-cyber.html>.

Value of Personally Identifiable Information

65. The Federal Trade Commission (“FTC”) defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.”¹² The FTC describes “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, among other things, “[n]ame, Social Security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.”¹³

66. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, Personal Information can be sold at a price ranging from \$40 to \$200, and bank details have a price range of \$50 to \$200.¹⁴ Experian reports that a stolen credit or debit card number can sell for \$5 to \$110 on the dark web.¹⁵ Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.¹⁶

67. Social Security numbers, for example, are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual’s Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

¹² 17 C.F.R. § 248.201 (2013).

¹³ *Id.*

¹⁴ *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital Trends, Oct. 16, 2019, *available at*: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last visited Jan. 19, 2022).

¹⁵ *Here’s How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last visited Jan 19, 2022).

¹⁶ *In the Dark*, VPNOverview, 2019, *available at*: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last visited Jan. 19, 2022).

A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.¹⁷

68. What's more, it is no easy task to change or cancel a stolen Social Security number.

An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

69. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."¹⁸

70. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security number, driver's license number, addresses, and financial information.

71. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information,

¹⁷ Social Security Administration, *Identity Theft and Your Social Security Number*, available at: <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited Jan. 19, 2022).

¹⁸ Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), available at: <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft> (last visited Jan. 19, 2022).

personally identifiable information and Social Security numbers are worth more than 10x on the black market.”¹⁹

72. Among other forms of fraud, identity thieves may use Social Security numbers to obtain driver’s licenses, government benefits, medical services, and housing or even give false information to police.

73. Driver’s license numbers are also incredibly valuable. “Hackers harvest license numbers because they’re a very valuable piece of information. A driver’s license can be a critical part of a fraudulent, synthetic identity – which go for about \$1200 on the Dark Web. On its own, a forged license can sell for around \$200.”²⁰

74. According to national credit bureau Experian:

A driver’s license is an identity thief’s paradise. With that one card, someone knows your birthdate, address, and even your height, eye color, and signature. If someone gets your driver’s license number, it is also concerning because it’s connected to your vehicle registration and insurance policies, as well as records on file with the Department of Motor Vehicles, place of employment (that keep a copy of your driver’s license on file), doctor’s office, government agencies, and other entities. Having access to that one number can provide an identity thief with several pieces of information they want to know about you.

Next to your Social Security number, your driver’s license number is one of the most important pieces of information to keep safe from thieves.²¹

75. According to cybersecurity specialty publication CPO Magazine, “[t]o those unfamiliar with the world of fraud, driver’s license numbers might seem like a relatively harmless

¹⁹ Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), available at: <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last visited Nov. 11, 2021).

²⁰ <https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3e4755c38658> (last accessed July 20, 2021).

²¹ Sue Poremba, *What Should I Do If My Driver’s License Number is Stolen?* (October 24, 2018) <https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/> (last accessed July 20, 2021).

piece of information to lose if it happens in isolation.”²² However, this is not the case. As cybersecurity experts point out:

“It’s a gold mine for hackers. With a driver’s license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification, or use the information to craft curated social engineering phishing attacks.”²³

76. Victims of driver’s license number theft also often suffer unemployment benefit fraud, as described in a recent New York Times article.²⁴

77. The fraudulent activity resulting from the Data Breach may not come to light for years.

78. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office (“GAO”), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.²⁵

79. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, including Social Security numbers, driver’s license numbers, and financial account information, and of the foreseeable consequences that would occur if Defendant’s data security system and network was breached,

²² <https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/> (last accessed July 20, 2021).

²³ *Id.*

²⁴ *How Identity Thieves Took My Wife for a Ride*, NY Times, April 27, 2021 <https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html> (last accessed July 20, 2021).

²⁵ *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: <https://www.gao.gov/assets/gao-07-737.pdf> (last visited Jan. 19, 2022).

including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

80. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

81. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to potentially thousands of individuals' detailed PII, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

82. In the breach notification letter, Defendant made an offer of 12 months of single bureau credit and identity monitoring services. This is wholly inadequate to compensate Plaintiff and Class Members as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' PII.

83. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

84. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers and financial information, fraudulent use of that information and damage to victims may continue for years.

Defendant Violated the Gramm-Leach-Bliley Act

85. Defendant is an accounting that provides tax and financial advice, and therefore is subject to the Gramm-Leach-Bliley Act (“GLBA”).

86. Defendant collects nonpublic personal information, as defined by 15 U.S.C. § 6809(4)(A), 16 C.F.R. § 313.3(n) and 12 C.F.R. § 1016.3(p)(1). Accordingly, during the relevant time period Defendant was subject to the requirements of the GLBA, 15 U.S.C. §§ 6801.1 et seq., and is subject to numerous rules and regulations promulgated on the GLBA Statutes. The GLBA Privacy Rule became effective on July 1, 2001. *See* 16 C.F.R. Part 313. Since the enactment of the Dodd-Frank Act on July 21, 2010, the Consumer Financial Protection Bureau (“CFPB”) became responsible for implementing the Privacy Rule. In December 2011, the CFPB restated the implementing regulations in an interim final rule that established the Privacy of Consumer Financial Information, Regulation P, 12 C.F.R. § 1016 (“Regulation P”), with the final version becoming effective on October 28, 2014.

87. Accordingly, Defendant’s conduct is governed by the Privacy Rule prior to December 30, 2011, and by Regulation P after that date.

88. Both the Privacy Rule and Regulation P require financial institutions to provide customers with an initial and annual privacy notice. These privacy notices must be “clear and conspicuous.” 16 C.F.R. §§ 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. “Clear and conspicuous means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice.” 16 C.F.R. § 313.3(b)(1); 12 C.F.R. § 1016.3(b)(1). These privacy notices must “accurately reflect[] [the financial institution’s] privacy policies and practices.” 16 C.F.R. § 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. They must include specified elements, including the categories of nonpublic personal information the

financial institution collects and discloses, the categories of third parties to whom the financial institution discloses the information, and the financial institution's security and confidentiality policies and practices for nonpublic personal information. 16 C.F.R. § 313.6; 12 C.F.R. § 1016.6. These privacy notices must be provided "so that each consumer can reasonably be expected to receive actual notice." 16 C.F.R. § 313.9; 12 C.F.R. § 1016.9. As alleged herein, Defendant violated the Privacy Rule and Regulation P.

89. Upon information and belief, Defendant failed to provide annual privacy notices to customers after the customer relationship ended, despite retaining these customers' PII and storing and/or sharing that PII on its network. Plaintiff has never received any privacy notice from Defendant.

90. Defendant failed to adequately inform its customers that it was storing and/or sharing, or would store and/or share, the customers' PII on its inadequately secured network and would do so after the customer relationship ended.

91. The Safeguards Rule, which implements Section 501(b) of the GLBA, 15 U.S.C. § 6801(b), requires institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (1) designating one or more employees to coordinate the information security program; (2) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks; (3) designing and implementing information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (4) overseeing service providers and requiring them by contract

to protect the security and confidentiality of customer information; and (5) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances. 16 C.F.R. §§ 314.3 and 314.4. As alleged herein, Defendant violated the Safeguard Rule.

92. Defendant failed to assess reasonably foreseeable risks to the security, confidentiality, and integrity of PII in its custody or control.

93. Defendant failed to design and implement information safeguards to control the risks identified through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

94. Defendant failed to adequately oversee service providers.

95. Defendant failed to evaluate and adjust its information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances.

Defendant Violated the FTC Act

96. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant’s duty in this regard.

97. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant’s conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff

and the Nationwide Class.

Plaintiff Spyro Stamat's Experience

98. Based upon the Notice of Data Breach letter that he received, Plaintiff's PII, including his name, address, Social Security Numbers, driver's license number, and other financial and tax information, was acquired, stored, and maintained by Defendant.

99. To date, GWLM has done next to nothing to adequately protect Plaintiff and Class Members, or to compensate them for their injuries sustained in this Data Breach.

100. Defendant's data breach notice letter downplays the theft of Plaintiff's and Class Members PII, when the facts demonstrate that the PII was targeted, accessed, and exfiltrated in a criminal cyberattack. The fraud and identity monitoring services offered by Defendant are only for one year, are not three-bureau monitoring, and place the burden squarely on Plaintiff and Class Members by requiring them to expend time signing up for the service and addressing timely issues when the service number for enrollment does not work properly.

101. Plaintiff and Class Members have been further damaged by the compromise of their PII.

102. Plaintiff Stamat's PII was compromised in the Data Breach, and was likely stolen and in the hands of cybercriminals who illegally accessed GWLM network for the specific purpose of targeting the PII.

103. Plaintiff Stamat typically takes measures to protect his PII, and is very careful about sharing his PII. Stamat has never knowingly transmitted unencrypted PII over the internet or other unsecured source.

104. Plaintiff Stamat stores any documents containing his PII in a safe and secure location, and he diligently chooses unique usernames and passwords for his online accounts.

105. As a result of the Data Breach, Plaintiff has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to this Data Breach. He has spent hours monitoring his accounts and credit scores as well as researching how he has been impacted by the Data Breach. In addition, Plaintiff has sustained emotional distress. This is time that was lost and unproductive and took away from other activities and duties.

106. Plaintiff also suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that he entrusted to Defendant for the purpose of obtaining services from Defendant, which was compromised in and as a result of the Data Breach.

107. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

108. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially his Social Security Number and driver's license being placed in the hands of criminals.

109. Defendant obtained and continues to maintain Plaintiff's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure. Plaintiff would not have entrusted his PII to Defendant had he known that it would fail to maintain adequate data security. Plaintiff's PII was compromised and disclosed as a result of the Data Breach.

110. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

CLASS ALLEGATIONS

111. Plaintiff brings this suit on behalf of himself and a class of similarly situated

individuals under Federal Rule of Civil Procedure 23, which is preliminarily defined as:

All persons GWLM identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach.

112. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

113. **Numerosity.** The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, public news reports indicate that approximately 18,515 individuals had their PII compromised in this Data Breach. The identities of Class Members are ascertainable through GWLM's records, Class Members' records, publication notice, self-identification, and other means.

114. **Commonality.** There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

- a. Whether GWLM unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;
- b. Whether GWLM failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- c. Whether GWLM data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- d. Whether GWLM data security systems prior to and during the Data Breach were

- consistent with industry standards;
- e. Whether GWLM owed a duty to Plaintiff and Class Members to safeguard their PII;
 - f. Whether GWLM breached its duty to Plaintiff and Class Members to safeguard their PII;
 - g. Whether computer hackers obtained Plaintiff's and Class Members' PII in the Data Breach;
 - h. Whether GWLM knew or should have known that its data security systems and monitoring processes were deficient;
 - i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of GWLM's misconduct;
 - j. Whether GWLM's conduct was negligent;
 - k. Whether GWLM's conduct was *per se* negligent, and;
 - l. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

115. **Typicality.** Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII, like that of every other Class member, was compromised in the Data Breach.

116. **Adequacy of Representation.** Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel is competent and experienced in litigating Class actions, including data privacy litigation of this kind.

117. **Predominance.** GWLM has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising

from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

118. **Superiority.** A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for GWLM. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

119. GWLM has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

120. Likewise, particular issues under Federal Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- a. Whether GWLM owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;
- b. Whether GWLM's security measures to protect their data systems were

reasonable in light of best practices recommended by data security experts;

- c. Whether GWLM's failure to institute adequate protective security measures amounted to negligence;
- d. Whether GWLM failed to take commercially reasonable steps to safeguard consumer PII; and
- e. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the data breach.

121. Finally, all members of the proposed Class are readily ascertainable. GWLM has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by GWLM.

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

122. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 121.

123. GWLM knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' PII, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

124. GWLM had a duty under common law to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' PII.

125. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

126. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members’ PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant’s duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

127. GWLM had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits “unfair. . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

128. GWLM, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class members by failing to exercise reasonable care in protecting and safeguarding Plaintiff’s and Class Members’ PII within GWLM’s possession.

129. GWLM, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff’s and Class Members’ PII.

130. GWLM, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiff and Class Members that the PII within GWLM’s possession might have been compromised and precisely the type of information compromised.

131. GWLM’s breach of duties owed to Plaintiff and Class Members caused Plaintiff’s and Class Members’ PII to be compromised.

132. As a result of GWLM's ongoing failure to notify Plaintiff and Class Members regarding the type of PII has been compromised, Plaintiff and Class Members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

133. GWLM's breaches of duty caused Plaintiff and Class Members to suffer from identity theft, loss of time and money to monitor their finances for fraud, and loss of control over their PII.

134. As a result of GWLM's negligence and breach of duties, Plaintiff and Class Members are in danger of imminent harm in that their PII, which is still in the possession of third parties, will be used for fraudulent purposes.

135. Plaintiff seeks the award of actual damages on behalf of himself and the Class.

136. In failing to secure Plaintiff's and Class Members' PII and promptly notifying them of the Data Breach, GWLM is guilty of oppression, fraud, or malice, in that GWLM acted or failed to act with a willful and conscious disregard of Plaintiff's and Class Members' rights. Plaintiff, therefore, in addition to seeking actual damages, seeks punitive damages on behalf of himself and the Class.

137. Plaintiff seeks injunctive relief on behalf of the Class in the form of an order compelling GWLM to institute appropriate data collection and safeguarding methods and policies with regard to patient information.

SECOND CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

138. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 121.

139. Defendant benefited from receiving Plaintiff's and Class Members' PII by its ability to retain and use that information for its own benefit. Defendant understood this benefit.

140. Defendant also understood and appreciated that Plaintiff's and Class Members' PII was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that information.

141. Plaintiff and Class Members conferred a monetary benefit upon Defendant in the form of providing (or having third-parties provide on their behalf) their PII to Defendant with the understanding that Defendant would pay for the administrative costs of reasonable data privacy and security practices and procedures. In exchange, Plaintiff and Class members should have received adequate protection and data security for such PII held by Defendant.

142. Defendant knew Plaintiff and Class members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiff and Class Members for business purposes.

143. Defendant failed to provide reasonable security, safeguards, and protections to the PII of Plaintiff and Class Members.

144. Under the principles of equity and good conscience, Defendant should not be permitted to retain money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures mandated by industry standards.

145. Defendant wrongfully accepted and retained these benefits to the detriment of Plaintiff and Class Members.

146. Defendant's enrichment at the expense of Plaintiff and Class Members is and was unjust.

147. As a result of Defendant's wrongful conduct, as alleged above, Plaintiff and the Class Members are entitled to restitution and disgorgement of all profits, benefits, and other compensation obtained by Defendant, plus attorneys' fees, costs, and interest thereon.

THIRD CAUSE OF ACTION
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

148. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 121.

149. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendant of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

150. Defendant violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect PII and not complying with industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII obtained and stored and the foreseeable consequences of a data breach on Defendant's systems.

151. GWLM's duty to use reasonable security measures also arose under the GLBA, under which GWLM was required to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards.

152. Defendant's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se*.

153. GWLM's violation of the GLBA and its Safeguards Rule constitutes negligence *per se*.

154. Class members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes), and the GLBA, were intended to protect.

155. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class Members. The GLBA, with its Safeguards Rule, was similarly intended.

156. As a direct and proximate result of Defendant GWLM's negligence, Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and Class Members, request judgment against Defendant and that the Court grant the following:

A. For an order certifying the Class, as defined herein, and appointing Plaintiff and his

Counsel to represent each such Class;

- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;
- C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:
 - i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
 - ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;
 - iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;
 - iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;
 - v. prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;
 - vi. requiring Defendant to engage independent third-party security

- auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
- vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;
 - viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;
 - ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;
 - x. requiring Defendant to conduct regular database scanning and securing checks;
 - xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;
 - xii. requiring Defendant to conduct internal training and education routinely and continually, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
 - xiii. requiring Defendant to implement a system of tests to assess its employees'

knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

- xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;
- xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential PII to third parties, as well as the steps affected individuals must take to protect themselves;
- xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

- D. For an award of damages, including actual, statutory, nominal, and consequential damages, as allowed by law in an amount to be determined;
- E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;
- F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

March 28, 2022

Respectfully, submitted,

s/Thomas Pacheco

Thomas Pacheco (Bar No. 21639)

**MILBERG COLEMAN BRYSON PHILLIPS
GROSSMAN, PLLC**

15453 Indianola Drive

Derwood, MD 20855

Telephone: (443) 980-6119

tpacheco@milberg.com

David K. Lietz*

**MILBERG COLEMAN BRYSON PHILLIPS
GROSSMAN, PLLC**

5335 Wisconsin Avenue NW

Suite 440

Washington, D.C. 20015-2052

Telephone: (866) 252-0878

Facsimile: (202) 686-2877

dlietz@milberg.com

Gary M. Klinger*

**MILBERG COLEMAN BRYSON PHILLIPS
GROSSMAN, PLLC**

227 W. Monroe Street, Suite 2100

Chicago, IL 60606

Phone: 866.252.0878

gklinger@milberg.com

Attorneys for Plaintiff and the Proposed Class

**Pro hac vice applications forthcoming*